REDUCED MORAL HAZARD AND STIGMA IMPACTS IN FORECASTING

Field Of The Invention

The present invention relates to forecasting, and more particularly to automation for forecasting the outcome of uncertain situations while avoiding conflicts of interests.

Background Of The Invention

Predicting future trends is an important task for almost all organizations. In order to make strategic decisions and plan for uncertain situations an organization will require a methodology and tool for forecasting that of the various possible outcomes is most likely. Forecasting of this type is required in a wide range of situations including production planning, evaluating technology, assessing the state of a market. As a result, a great deal of time and money is spent in these forecasts.

Committees of experts or consultants, and statistical inference techniques are conventional. More recently, information is treated as an asset that can be traded within a market in the form of state contingent securities. Such techniques have been found to be relatively accurate when compared to the traditional methods of predicting outcomes in uncertain situations.

United States Patent Application, US 2003/0078829 A1, by Chen et al., describes predicting future outcomes using an information market in which predictions for a group of forecaster's are accumulated with adjustments that account for each individual participants characteristics. But such does not address the problem that those directly involved in predicting future outcomes used in a forecast will have a conflict of interest in participating in the forecasting process.

In general, a conflict of interest exists in a situation in which an individual is making a prediction about an uncertain outcome and they can personally benefit by their prediction. An ethical line is crossed if they influence the actual outcome that is the subject of the prediction.

Clearly in this situation the individual can influence the outcome to try and attain their prediction in order to receive the reward for accurate prediction. If an individual's prediction is higher than predicted by others the conflict of interest situation can have positive affects, in which in order for the company or organization to meet the predicted outcome the organization is pushed to work harder or more efficiently. On the other hand when the individual has made a pessimistic forecast they may relax their standards and slow production or take other detrimental action so as to meet their prediction. A conflict of interest of this type is often termed a moral hazard.

Another pervasive problem in a real world situation that influences the success of any predictive tool is the willingness for people to participate in the prediction process. In a situation in which either a perceived or real moral hazard situation is likely to occur, participation in forecasting is less likely. Moreover the stigma associated with publicly making negative predictions about ones colleagues or workers may be a further disincentive to participate in forecasting activities.

Summary Of The Invention

Briefly, a forecasting system embodiment of the present invention comprises a plurality of forecasters that provide predictions and that have individual identities. A plurality of users depend on receiving the predictions from the forecasters and use forecasts assembled there from to manage a business organization. An encryption system encodes and hides the individual identities of each of the plurality of forecasters and thereby encourages more honest predictions. A decryption system decodes and reveals the individual identities of each of the plurality of forecasters and discourages moral hazards in the predictions. The individual identities of each of the plurality of forecasters are encrypted, associated, and embedded with their respective predictions.

Brief Description Of The Drawings

Fig. 1 is a functional block diagram of a computer system embodiment of the present invention for generating forecasts;

Fig. 2 is a flowchart diagram of a forecasting process embodiment of the present invention;

Fig. 3 is a flowchart diagram of another forecasting process embodiment of the present invention;

Fig. 4 is a dataflow diagram of an identity escrow embodiment of the invention in which the entities are all members of the production group;

Fig. 5 is a dataflow diagram of an alternative identity escrow scheme that can be used wherein the entities include the members of the production group and the organization for that the forecasts are being provided;

Fig. 6 is a graph of the equilibrium states for participation and defection in respect of forecasting and production that can be used to optimize the design choices available when implementing a method according to the present invention; and

Fig. 7 is a graph similar to that of Fig. 6 but for an alternative embodiment of the invention.

Detailed Description Of The Embodiments

A forecasting embodiment of the present invention maybe implemented by software hosted on a computer system and network. An exemplary forecast network 100 is shown in Fig. 1. Embodiments of the present invention provide forecasts based on anonymous forecasting and enable group detection of bias. The anonymous forecasting encourages legitimate forecasting of negative outcomes, and such group detection of bias reduces the likelihood that a forecaster could run amok. Conditional anonymity is provided to each forecaster. The relative privacy offered by the process enables pessimistic forecasts to be made

without incurring a social cost associated with announcing a pessimistic forecast, whilst the threat of a loss of privacy deters the establishment of detrimental conflicts of interest.

The forecasting network 100 includes a server 101 with a memory 102, a database 104, and a processor 106. In use, the processor 106 is configured to run a forecasting application program that is loaded into the computer memory 102. Computer memory 102 stores forecast data and other data generated by or received by the computer system. Memory 104 has stored therein one or more database structures for storing data created by the processor 106 and received from forecasters or entities, including forecast data, encryption data, decryption keys or decryption elements.

Server 101 networks through a connection 108 to the Internet or other computer network 110. A forecaster 112 is connected to network 110 by communications link 114, and a group 116 of entity systems 118, 120, and 122 are connected to the network 110 by respective communication links 124, 126, and 128.

A business organization needing forecasting may be hierarchically organized into production groups of various sizes. Each production group typically has a designated person associated with it that provides a prediction for the output of the production group. Often, this forecaster is the group manager or one of the members of the production group. In certain organizations, more than one person may make predictions for the output of the production group.

For example, forecaster 112 is associated with a organization production group to enter forecast data and forward

it to server 101. The forecaster 112 runs an application program that allows data communication with server 101, e.g., Internet browser application communicating with a webpage hosted on server 101. Alternatively, the application program running on the forecaster system 112 may be a dedicated application that allows entry of predictions in accordance with a predetermined data format for transmission to server 101.

Each of the members, or entities, of the production group can access any one of the entity systems group 116. These each include an application program that allows data to be exchanged with server 101, such as an Internet browser. A webpage on server 101 allows a production group member to submit a request to server 101 for forecast data. The webpage may be implemented in the form of an on-line form that contains data entry fields that enable the entity to enter text identifying a suspect forecast or forecaster.

The organization's management uses forecasts for strategic business planning. If a moral hazard is suspected, e.g., a conflict of interest, a request may be made to server 101. Entity systems 118, 120, and 122 can ask for forecasting details including the specific identity of the forecasters. Otherwise, the forecasters' identities are concealed to encourage candid and honest forecasts.

Fig. 2 represents a forecasting process embodiment of the present invention, and is referred to herein by the general reference numeral 200. Process 200 includes a step 202 in which, e.g., server 101 (Fig. 1) receives a prediction from a forecaster. Typically, such will be in response by forecasters

112 to a web-page being sent asking them to predict something, e.g., the production output of their respective production group for the next month. For simplicity, forecasting network 100 in Fig. 1 is shown as only having one forecaster 112. Each forecaster 112 responds by transmitting a prediction, the forecaster's identity, and any comments. Many forecasters will provide individual forecast data.

The predictions received for each production group are accumulated into a single global prediction. These are stored, e.g., in database 104, for later broadcast to the organization. The reporting of forecasts is done anonymously. The organization does not know which of the received forecasts relates to that production group, and consequently which forecaster made such prediction. In this way, the organization gets the benefit of the forecasting procedure, and the individuals do not risk some of the stigma that could occur if reporting negative feedback to their superiors.

Once the forecast data has been received by the computer system and production or other organizational activities are underway that is aimed at achieving an outcome in relation to the uncertain situation, there is the possibility that one or more members of the production group will suspect that the forecaster for their production group has provided a negative forecast for the group and is attempting to influence the operation of the group to meet their prediction.

In a step 204, the members of the production group can submit a request to disclose a forecaster's identity if a moral hazard is suspected. An interactive webpage or application

program can be used to make such a request. A step 206 asks if the request to disclose has come from a proper subgroup of users. If not, control passes to a step 208. Otherwise, the requested disclosure in made in a step 210.

In most implementations the members of the production group will know who makes the forecasts for their group, so such forecasting is not anonymous. However, when the forecasting is secret, the production group is not told the forecast made in relation to their group. They must detect a moral hazard from the behavior, without knowing the prediction.

In step 206, the processor determines if requests to disclose forecast data have been received from a subgroup of the members of the production group, indicating that they suspect a moral hazard. A moral hazard is more likely when the number of requests received in step 204 is high. The subgroup may include a variety of members of the organization, the production group, etc.

In a one embodiment, threshold cryptography is used to conditionally protect the forecast data. The forecast data, the forecaster's identity, and predictions, are encrypted by the processor using a public key and stored, e.g., in the database 104 (Fig. 1). A private key is required to decrypt the forecast data and disclose the forecaster's identity and prediction.

In threshold cryptography, the private key is divided into several pieces. Each key part is distributed to various individuals in a subgroup. Here in this example, a piece of the private key associated with each of the members of the

production group is stored in database 104. When a request is received from an individual, a piece of the whole private key is provided to the processor to use in the decryption process. At least *k* number of pieces are required to reconstruct a whole private key. If their are k pieces, the identity of the person who made the suspicious prediction will become accessible.

Embodiments of the present invention are such that when a sufficient number of requests for disclosure have been received, there will be sufficient decryption key segments to be able decrypt the forecast data.

A method embodiment of the present invention is illustrated in Fig. 3, and is referred to herein by the general reference numeral 300. Method 300 begins with a step 302 in which forecast data is received and stored. Such data includes a forecast and an encrypted payload. The forecaster's identity is included in the encrypted payload and is accessible when a threshold number of private key segments are on hand to unlock it. A step 304 encrypts the forecast data. A step 306 associates each of the private key segments with a corresponding group member. A minimum number of these private key segments will need to be gathered together later to decrypt the encoded data if that becomes necessary. Until decrypted, the forecasts related to the encrypted forecast data are publicly accessible and anonymous.

In a particular embodiment, the decryption elements are stored in the database. Such are forwarded to the processor for use in decryption after a request is received from the entity associated with a key. Alternatively, the decryption elements

can be transmitted to the entity systems. In such an implementation, a request to disclose forecast data includes transmission of a decryption element to the computer system.

Next, in a step 308, the requests to disclose forecast data are received from the entities within the group. In a step 310, the processor is provided with the corresponding decryption elements in response to the received requests. The decryption elements can be provided from the database, or as part of the request data. In an alternative embodiment, the request data may not include the decryption element. The processor can request transmission of the decryption element that is stored on the entity computer system upon receipt of a request.

In a step 312, the processor determines whether a threshold number of decryption elements have been received. If so, a step 314 decrypts the requested forecast data. Otherwise, a step 316 refuses to decrypt the forecast data. A step 318 sends the decrypted data to the requestors.

Fig. 4 represents a threshold cryptography process embodiment of the present invention, and is referred to herein by the general reference numeral 400. A forecaster's identity 402, and a forecaster's prediction 404, are associated by the processor and stored as forecast data 406. A step 408 encrypts the paired information. The encryption algorithm used is unlocked by a private key 410. Such is divided in a step 412, e.g., into constituent parts 414, 416, 418.

Individually, none of the constituent parts 414, 416, and 418, can be used to access any information regarding the identity of the forecaster or the other encrypted elements.

However, when a threshold number of the constituent parts 414, 416, and 418, are available, the associated private encryption key 420 can be reconstructed and the forecaster's identity and prediction revealed. Each of the constituent parts 414, 416, and 418, is provided to, or associated with, a respective one of a production group member 420, 422, and 424.

Fig. 5 represents a variation on process 400 (Fig. 4). The associated private encryption key is divided differently. The division method shown in Fig. 5 can advantageously be used with an identity escrow scheme such that the organization is given the opportunity to participate in the decision whether to reveal the forecast and identity of a suspicious forecaster. The organization alone is unable to decrypt a forecaster's identity. A minimum number of constituent parts of the private key are needed to be contributed by production group members. The division and distribution of the private encryption key can be such as to increase the number of key segments given to the organization. For example, to increase the ability of the organization to reveal the identity of a forecaster.

Fig. 5 represents a threshold cryptography process embodiment of the present invention, and is referred to herein by the general reference numeral 500. A forecaster's identity 502, and a forecaster's prediction 504, are associated by the processor and stored as forecast data 506. A step 508 encrypts the paired information. The encryption algorithm used is unlocked by a private key 510. Constituent parts 512, 514, 516, and 518, are divided up in a step 520.

Individually, none of the constituent parts 512, 514, 516, and 518, can be used to access any information regarding the identity of the forecaster or the other encrypted elements. However, when a threshold number of the constituent parts 512, 514, 516, and 518, are available, the associated private encryption key 510 can be reconstructed and the forecaster's identity and prediction revealed. Each of the constituent parts 512, 514, 516, and 518, is provided to, or associated with, a respective one of a production group member 522, 524, and 526, and importantly also to organization 528.

Once the forecaster's identity and forecast is revealed and any other associated information that has also been stored in relation to the forecast is reviewed it can be determined whether the particular person was actually acting against the interest of the organization or not.

In one method embodiment, all of the members of the production group must suspect a moral hazard for the suspicious forecast to be revealed, that is, the threshold number of members of the production group required to reveal a forecast is equal to the size of the production group. In this implementation the reconstitution of the private encryption key is relatively straightforward, with the only complicating factor being that a subgroup of the production group smaller than the whole must not be able to either ascertain the remaining parts of the private encryption key or otherwise decrypt the forecast data without all members providing their segment of the private encryption key.

In the embodiment a threshold cryptography algorithm is used that has the property that at least k members of the group of size n are required to reconstruct the private key and that any subgroups smaller than k individuals obtains no information at all about the key or the encrypted forecast data. In this example $k < n$.

TABLE II

A suitable method of key splitting is operates in the following manner.

1. The public key identifying an individual forecaster is expressed as a secret integer I, where $I > 0$ and is distributed amongst the n members of the production group.

2. A prime p is chosen such that $p > I$ and a coefficient a_0 is defined as $a_0 = I$.

3. $t - 1$ random, independent coefficients $a_1, \ldots a_{t-1}$ are selected such that $0 \le a_j \le (p-1)$ to define a random polynomial $f(x) = \sum a_j x^j$.

4. Compute $I_i = f(i) \bmod p$, $1 \le i \le n$ (or for any n distinct points i, $1 \le i \le (p-1)$). Each piece I_i is securely transferred to a respective production group member P_i along with the public index i.

5. Any group of t or more members of the production group can combine their pieces of the polynomial thus providing t

distinct points $(x,y)=(i,I_i)$. Computing the coefficients a_j of $f(x)$where, $1 \le j \le (t-1)$, using the Lagrange interpolation scheme. The secret identity can be recovered by noting that $f(0) = a_0 = I$, that is the encrypted secret integer.

In such technique, the coefficients of an unknown polynomial $f(x)$ of degree t defined by the set of points (x_i, y_i) where $1 \le i \le t$, are given by the Lagrange interpolation formula:

$$f(x)=\sum_{i=1}^{n}\prod_{1\le j}\frac{(x-x_j)}{(x_i-x_j)} \quad .$$

Since $f(0) = a_0 = I$, the secret identity I can be expressed as;

$$I=\sum_{i=1}^{n}c_i y_i$$

where,

$$c_i=\prod_{1\le j\le t}\frac{x_j}{(x_j-x_i)} \quad .$$

Thus the production group can compute I as a linear combination of t pieces y_i since the coefficients c_i are non-secret constants.

Thus, in this embodiment the decryption elements transmitted to or otherwise associated with each entity can take